

AN EQUIVALENCE RELATION ON A SET OF WORDS OF FINITE LENGTH

YOTSANAN MEEMARK AND TASSAWEE THITIPAK

ABSTRACT. In this work, we study several equivalence relations induced from the partitions of the sets of words of finite length. We have results on words over finite fields extending the work of Bacher (2002, Europ. J. Combinatorics, **23**, 141-147). Cardinalities of its equivalence classes and explicit relationships between two words are determined. Moreover, we deal with words of finite length over the ring $\mathbb{Z}/N\mathbb{Z}$ where N is a positive integer. We have arithmetic results parallel to Bacher's.

1. INTRODUCTION

Let k be a finite field and F_k denote the set of all finite words with letters in k . F_k is a free monoid with identity ε , called the *empty word*. Consider the special linear group of degree two over k , $\mathrm{SL}_2(k)$, consisting of 2×2 matrices over k of determinant one. It has been proved in [B02] Lemma 2.1 that $\mathrm{SL}_2(k)$ generated as a monoid by the set of matrices

$$S = \left\{ \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} : \alpha \in k \right\}.$$

We can view S as k and thus every word $w = \alpha_1 \dots \alpha_l \in F_k$ is corresponding to the product

$$\begin{bmatrix} 0 & 1 \\ -1 & \alpha_1 \end{bmatrix} \dots \begin{bmatrix} 0 & 1 \\ -1 & \alpha_l \end{bmatrix} \in \mathrm{SL}_2(k).$$

2000 *Mathematics Subject Classification*. Primary: 20G40; Secondary: 05E15.

Key words and phrases. Equivalence relations; SL_2 ; Words.

The research of the first author was supported in part by Grants for Development of New Faculty Staff from Chulalongkorn University, Thailand. This work grows out of the second author's master thesis at Chulalongkorn university written under the direction of the first author to which the second author expresses his gratitude.

This gives rise to an onto homomorphism of monoids

$$\pi : F_k \rightarrow \mathrm{SL}_2(k).$$

We define an equivalence relation \sim on $k^2 \setminus \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}$ by

$$\begin{bmatrix} s \\ t \end{bmatrix} \sim \begin{bmatrix} u \\ v \end{bmatrix} \Leftrightarrow \begin{bmatrix} s \\ t \end{bmatrix} = \lambda \begin{bmatrix} u \\ v \end{bmatrix} \text{ for some } \lambda \in k^\times.$$

Its equivalence classes are the lines spanned by $\begin{bmatrix} 1 \\ x \end{bmatrix}$, $x \in k$, and the line spanned by $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, called the *infinite line*, with the origin deleted. Then we usually write these classes as $\begin{bmatrix} 1 \\ x \end{bmatrix}$, $x \in k$, and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Thus the set of all equivalence classes, denoted by $\mathbb{P}^1(k)$ and called the *projective 1-space*. The group $\mathrm{SL}_2(k)$ acts on $\mathbb{P}^1(k)$ by left multiplication. Bacher defined the subset \mathcal{A} of F_k by

$$\mathcal{A} = \left\{ w \in F_k : \pi(w) \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\}.$$

The sets \mathcal{A} and $\mathcal{C} = F_k \setminus \mathcal{A}$ divide F_k into two disjoint pieces. This partition leads to an equivalence relation on F_k .

For $r \in k$, we define two disjoint subsets \mathcal{A}_r and \mathcal{C}_r of F_k by

$$\mathcal{A}_r = \left\{ w \in F_k : \pi(w) \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ r \end{bmatrix} \right\}.$$

and $\mathcal{C}_r = F_k \setminus \mathcal{A}_r$. Hence $\mathcal{A} = \mathcal{A}_0$. In Sections 2 and 3, we investigate arithmetic and combinatorial properties of the equivalence relation on F_k induced by the partition \mathcal{A}_r and \mathcal{C}_r .

Let N be a positive integer. Another route to extend Bacher's work is to study the special linear group over $\mathbb{Z}/N\mathbb{Z}$, the ring of integers modulo N . We present this topic in Section 4. Write F_N for the set of all finite words with letters in $\mathbb{Z}/N\mathbb{Z}$. Consider the special linear group of degree two over $\mathbb{Z}/N\mathbb{Z}$, $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, consisting of 2×2 matrices

over $\mathbb{Z}/N\mathbb{Z}$ of determinant one. Let

$$S' = \left\{ \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} : \alpha \in \mathbb{Z}/N\mathbb{Z} \right\}.$$

We show that this set generates $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ as a monoid. Our proof is different from [B02] Lemma 2.1. We use the basic fact that every closed subset of a finite group is a group. This result shows that every element of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ can be written in at least one way as a finite word with letters in S' .

We can also consider S' as $\mathbb{Z}/N\mathbb{Z}$ and hence every word $w = \alpha_1 \dots \alpha_l \in F_N$ is corresponding to the product

$$\begin{bmatrix} 0 & 1 \\ -1 & \alpha_1 \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ -1 & \alpha_l \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

This yields an onto homomorphism of monoids

$$\pi : F_N \rightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

For $\mathbb{Z}/N\mathbb{Z}$, we define an equivalence relation \sim' on $(\mathbb{Z}/N\mathbb{Z})^2 \setminus \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}$ by

$$\begin{bmatrix} s \\ t \end{bmatrix} \sim' \begin{bmatrix} u \\ v \end{bmatrix} \Leftrightarrow \begin{bmatrix} s \\ t \end{bmatrix} = \lambda \begin{bmatrix} u \\ v \end{bmatrix} \text{ for some } \lambda \in (\mathbb{Z}/N\mathbb{Z})^\times.$$

Here $(\mathbb{Z}/N\mathbb{Z})^\times$ denotes the unit group of the ring $\mathbb{Z}/N\mathbb{Z}$. The group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on the set of equivalence classes by left multiplication. Parallel to Bacher's, we set

$$\bar{\mathcal{A}} = \left\{ w \in F_N : \pi(w) \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\}$$

and $\bar{\mathcal{C}} = F_N \setminus \bar{\mathcal{A}}$. We study this partition of F_N in the last two sections.

The paper is organized as follows. Arithmetic and combinatorial properties implying the cardinalities of \mathcal{A}_r and \mathcal{C}_r are studied in Section 2. Section 3 gives an algorithm to distinguish the partition \mathcal{A}_r and \mathcal{C}_r . Words over $\mathbb{Z}/N\mathbb{Z}$ and the partition $\bar{\mathcal{A}}$ and $\bar{\mathcal{C}}$ are presented in Section 4. The final section is devoted to $\bar{\mathcal{A}}$ including unique factorization, predecessors, successors and periodic words, parallel to Bacher's \mathcal{A}_0 .

2. CARDINALITIES OF \mathcal{A}_r AND \mathcal{C}_r

This section presents the preliminary properties of words in \mathcal{A}_r and results on the cardinalities of \mathcal{A}_r and \mathcal{C}_r .

For $w \in F_k$ with $\pi(w) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(k)$, we note that

$$\begin{aligned} w \in \mathcal{A}_r &\Leftrightarrow \begin{bmatrix} 1 \\ r \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} b \\ d \end{bmatrix} \Leftrightarrow d = br \\ &\Leftrightarrow \pi(w) = \begin{bmatrix} a & b \\ ar - b^{-1} & br \end{bmatrix} \text{ with } a \in k, b \in k^\times. \end{aligned}$$

Therefore we have shown

Theorem 2.1. *For $r \in k$,*

$$\mathcal{A}_r = \left\{ w \in F_k : \pi(w) = \begin{bmatrix} a & b \\ ar - b^{-1} & br \end{bmatrix} \text{ for some } a \in k, b \in k^\times \right\}.$$

The set \mathcal{A}_0 has been studied by Bacher in [B02]. Our results are for the case $r \neq 0$. For $l \geq 0$, we write F_k^l for the set of words over k of length l , $\mathcal{A}_r^l = F_k^l \cap \mathcal{A}_r$ and $\mathcal{C}_r^l = F_k^l \cap \mathcal{C}_r$. Unless specify, we assume $r \in k^\times$ throughout this section. We begin with the right insertion.

Theorem 2.2. *Let $w \in F_k$. Then $w \in \mathcal{A}_r^l$ if and only if $w\alpha \in \mathcal{C}_r^{l+1}$ for all $\alpha \in k$. Moreover, if $w \in \mathcal{C}_r^l$, then there exists a unique $\alpha \in k$ such that $w\alpha \in \mathcal{A}_r^{l+1}$.*

Proof. Assume that $w \in \mathcal{A}_r^l$ and let $\alpha \in k$. Then $\pi(w) = \begin{bmatrix} a & b \\ ar - b^{-1} & br \end{bmatrix}$ for some $a \in k$ and $b \in k^\times$. Thus

$$\pi(w\alpha) = \pi(w)\pi(\alpha) = \begin{bmatrix} a & b \\ ar - b^{-1} & br \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} = \begin{bmatrix} -b & a + \alpha b \\ -br & ar - b^{-1} + \alpha br \end{bmatrix}.$$

If $ar - b^{-1} + \alpha br = (a + \alpha b)r$, then $-b^{-1} = 0$, a contradiction. Thus $w\alpha \in \mathcal{C}_r^{l+1}$. Conversely, suppose that $w \in \mathcal{C}_r^l$. Then $\pi(w) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(k)$ and $d \neq br$. Note that for $\alpha \in k$,

we have

$$\pi(w\alpha) = \pi(w)\pi(\alpha) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} = \begin{bmatrix} -b & a + \alpha b \\ -d & c + \alpha d \end{bmatrix}.$$

Since $d \neq br$, we can choose a unique α , namely $\alpha = (ar - c)(d - br)^{-1} \in k$ such that $\pi(w\alpha) = \begin{bmatrix} -b & (d - br)^{-1} \\ -d & r(d - br)^{-1} \end{bmatrix}$ and hence $w\alpha \in \mathcal{A}_r^{l+1}$. \square

For the left insertion, we obtain a slightly different property.

Theorem 2.3. *Let $w \in F_k$ with $\pi(w) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(k)$.*

- (i) *If $w \in \mathcal{C}_r^l$, then $d = 0$ if and only if $\alpha w \in \mathcal{C}_r^{l+1}$ for all $\alpha \in k$.*
- (ii) *If $w \in \mathcal{A}_r^l$, then there exists a unique $\alpha \in k$ such that $\alpha w \in \mathcal{A}_r^{l+1}$.*

Proof. We first observe that for $\alpha \in k$,

$$\pi(\alpha w) = \pi(\alpha)\pi(w) = \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ -a + \alpha c & -b + \alpha d \end{bmatrix}.$$

- (i) Assume that $w \in \mathcal{C}_r^l$. If $d = 0$, then $b \neq 0$, so $\pi(\alpha w) = \begin{bmatrix} c & 0 \\ -a + \alpha c & -b \end{bmatrix}$ which means $\alpha w \in \mathcal{C}_r^{l+1}$. If $d \neq 0$, then there exists $\alpha = (b + dr)d^{-1}$ such that $\pi(\alpha w) = \begin{bmatrix} c & d \\ -d^{-1} + cr & dr \end{bmatrix}$ which implies $\alpha w \in \mathcal{A}_r^{l+1}$.
- (ii) Assume that $w \in \mathcal{A}_r^l$. Then $d = br$. A simple calculation yields a unique $\alpha = r + r^{-1}$ such that $\pi(\alpha w) = \begin{bmatrix} c & br \\ -a + c(r + r^{-1}) & br^2 \end{bmatrix}$ which means $\alpha w \in \mathcal{A}_r^{l+1}$. \square

Next we present results on left and right deletions of a word $w \in \mathcal{A}_r$.

Theorem 2.4. *Let $\alpha_1 \dots \alpha_l \in \mathcal{A}_r^l$. Then $\alpha_1 \dots \alpha_{l-1} \in \mathcal{C}_r^{l-1}$, and $\alpha_2 \dots \alpha_l \in \mathcal{A}_r^{l-1}$ if and only if $\alpha_1 = r + r^{-1}$.*

Proof. Assume that $\alpha_1 \dots \alpha_l \in \mathcal{A}_r^l$. Then $\pi(\alpha_1 \dots \alpha_l) = \begin{bmatrix} a & b \\ ar - b^{-1} & br \end{bmatrix}$ for some $a \in k$ and $b \in k^\times$. Thus

$$\begin{aligned} \pi(\alpha_1 \dots \alpha_{l-1}) &= \pi(\alpha_1 \dots \alpha_l) \pi(\alpha_l)^{-1} = \begin{bmatrix} a & b \\ ar - b^{-1} & br \end{bmatrix} \begin{bmatrix} \alpha_l & -1 \\ 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} \alpha_l a + b & -a \\ \alpha_l(ar - b^{-1}) + br & b^{-1} - ar \end{bmatrix}. \end{aligned}$$

Since $b^{-1} \neq 0$, $b^{-1} - ar \neq -ar$ and so $\alpha_1 \dots \alpha_{l-1} \in \mathcal{C}_r^{l-1}$. Hence

$$\begin{aligned} \pi(\alpha_2 \dots \alpha_l) &= \pi(\alpha_1)^{-1} \pi(\alpha_1 \dots \alpha_l) = \begin{bmatrix} \alpha_1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ ar - b^{-1} & br \end{bmatrix} \\ &= \begin{bmatrix} \alpha_1 a - ar + b^{-1} & \alpha_1 b - br \\ a & b \end{bmatrix}. \end{aligned}$$

Therefore $\alpha_2 \dots \alpha_l \in \mathcal{A}_r^{l-1} \Leftrightarrow b = (\alpha_1 b - br)r \Leftrightarrow \alpha_1 = r + r^{-1}$. \square

Theorem 2.2 results in $|\mathcal{A}_r^{l+1}| \geq |\mathcal{C}_r^l|$ and Theorem 2.4 (i) gives rise to $|\mathcal{A}_r^{l+1}| \leq |\mathcal{C}_r^l|$. Thus $|\mathcal{A}_r^{l+1}| = |\mathcal{C}_r^l|$. Since $|\mathcal{A}_r^l| + |\mathcal{C}_r^l| = q^l$, we get the recurrence relation

$$|\mathcal{A}_r^{l+1}| + |\mathcal{A}_r^l| = q^l \text{ for } l \geq 0 \quad \text{and} \quad |\mathcal{A}_r^0| = 0.$$

Solving this relation, we obtain the cardinalities of \mathcal{A}_r^l and \mathcal{C}_r^l for all $l \geq 0$. It should be pointing out that Bacher had the same numbers for $r = 0$ in [B02] Corollary 2.3. We record this result in

Corollary 2.5. *For a finite field k with q elements, $l \geq 0$ and $r \in k$, we have*

$$|\mathcal{A}_r^l| = \frac{q^l - (-1)^l}{q + 1} \quad \text{and} \quad |\mathcal{C}_r^l| = \frac{q^{l+1} + (-1)^l}{q + 1}.$$

3. INDUCED EQUIVALENCE RELATIONS

Let $r \in k$. The partition \mathcal{A}_r and \mathcal{C}_r of F_k induces the equivalence relation \sim_r on F_k . Its properties are studied in our next theorem.

Theorem 3.1. *Let $x \in F_k$ and $\beta \in k$. We have*

- (i) *If $\alpha \in k$ and $\alpha \neq r$, then $\alpha\beta x \sim_r \gamma x$ where $\gamma = \frac{r^2 - (\alpha - \beta)r + 1 - \alpha\beta}{r - \alpha}$.*
- (ii) *$r\beta x \in \mathcal{A}_r$ if and only if $x \in \mathcal{A}_0$.*

Proof. Let $\pi(x) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(k)$.

- (i) Assume that $\alpha, \beta \in k$ and $\alpha \neq r$. Then

$$\pi(\alpha\beta x) = \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \beta \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a + \beta c & -b + \beta d \\ -\alpha a - c + \alpha\beta c & -\alpha b - d + \alpha\beta d \end{bmatrix}$$

and

$$\pi(\gamma x) = \begin{bmatrix} 0 & 1 \\ -1 & \gamma \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ -a + \gamma c & -b + \gamma d \end{bmatrix}.$$

Thus

$$\begin{aligned} \alpha\beta x \in \mathcal{A}_r &\Leftrightarrow (-b + \beta d)r = -\alpha b - d + \alpha\beta d \\ &\Leftrightarrow -br + \beta dr = -\alpha b - d + \alpha\beta d \\ &\Leftrightarrow dr^2 - \alpha dr = -br + \alpha b + dr^2 - (\alpha - \beta)dr + (1 - \alpha\beta)d \\ &\Leftrightarrow dr = -b + \frac{(r^2 - (\alpha - \beta)r + 1 - \alpha\beta)}{r - \alpha}d, \end{aligned}$$

so $\alpha\beta x \sim_r \gamma x$ where $\gamma = \frac{(r^2 - (\alpha - \beta)r + 1 - \alpha\beta)}{r - \alpha}$.

- (ii) Since $\pi(r\beta x) = \begin{bmatrix} 0 & 1 \\ -1 & r \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \beta \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a + \beta c & -b + \beta d \\ -c - ar + \beta rc & -d - br + \beta rd \end{bmatrix}$, $r\beta x \in \mathcal{A}_r \Leftrightarrow (-b + \beta d)r = -d - br + \beta rd \Leftrightarrow d = 0 \Leftrightarrow x \in \mathcal{A}_0$. \square

Remark. This result leads to an algorithm to distinguish words in F_k . It extends Bacher's work on \sim_0 in [B02] Proposition 2.4 (ii) to $\sim_r, r \in k$. Note that $\alpha \sim_r \varepsilon \Leftrightarrow \alpha \neq r$. Combined with Theorem 3.1, we completely classify all words into the partition \mathcal{A}_r and \mathcal{C}_r of F_k .

We illustrate Theorem 3.1 and the above remark by the following numerical example.

Example 3.2. Let $k = \mathbb{F}_3$. Consider $22102 \in F_k$.

$r = 0$. By Theorem 3.1 (i), $22102 \sim_0 (2 - 2^{-1})102 = 0102$. By Theorem 3.1 (ii), $0102 \sim_0 02 \sim_0 \varepsilon$. Then we have $22102 \in \mathcal{C}_0$.

$r = 1$. By Theorem 3.1 (i),

$$\begin{aligned} 22102 &\sim_1 \left[\frac{1^2 - (2 - 2)1 + 1 - 2 \cdot 2}{1 - 2} \right] 102 = 2102 \\ &\sim_1 \left[\frac{1^2 - (2 - 1)1 + 1 - 2 \cdot 1}{1 - 2} \right] 02 = 102. \end{aligned}$$

Since $2 \in \mathcal{C}_0$, $102 \in \mathcal{C}_1$ by Theorem 3.1 (ii). Then we have $22102 \in \mathcal{C}_1$.

$r = 2$. By Theorem 3.1 (ii), we first consider

$$102 \sim_0 (0 - 1^{-1})2 = 22 \sim_0 (2 - 2^{-1})\varepsilon = 0.$$

Then $102 \in \mathcal{A}_0$, so we have $22102 \in \mathcal{A}_2$.

4. WORDS OVER $\mathbb{Z}/N\mathbb{Z}$

In this section, we study arithmetic properties of the partition $\bar{\mathcal{A}}$ and $\bar{\mathcal{C}}$ of the set F_N defined parallel to Bacher's. Let

$$S' = \left\{ \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} : \alpha \in \mathbb{Z}/N\mathbb{Z} \right\}.$$

We begin by giving the proof of the following lemma.

Lemma 4.1. *The set S' generates $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ as a semigroup.*

Proof. Recall Theorem 2 in Chapter VII of Serre's book [S73] that the set of matrices $\left\{ \begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}$ generates $\mathrm{SL}_2(\mathbb{Z})$ as a group. Since the map $\mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ obtained by reducing the matrix entries modulo N is a surjective group homomorphism. Then $\left\{ \begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\} \pmod{N}$ also generates $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ as a group.

Consider $\langle S' \rangle$, a semigroup generated by S' . Since $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is finite, $\langle S' \rangle$ is a finite closed subset of $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})$, so it is a subgroup. Note that $\langle S' \rangle$ contains both generators $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $\begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ of $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Hence $\langle S' \rangle = \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$. \square

This lemma shows that every element of $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ can be written in at least one way as a finite word with letters in S' .

Next, we establish a way to determine if words are in $\bar{\mathcal{A}}$. For $w \in F_N$ with $\pi(w) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$, we note that

$$\begin{aligned} w \in \bar{\mathcal{A}} &\Leftrightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} b \\ d \end{bmatrix} \Leftrightarrow d = 0 \\ &\Leftrightarrow \pi(w) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} \text{ with } a \in \mathbb{Z}/N\mathbb{Z}, b \in (\mathbb{Z}/N\mathbb{Z})^\times. \end{aligned}$$

Hence we have shown

Theorem 4.2. *Let N be a positive integer. Then*

$$\bar{\mathcal{A}} = \left\{ w \in F_N : \pi(w) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} \text{ for some } a \in \mathbb{Z}/N\mathbb{Z}, b \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

For $l \geq 0$, we write F_N^l for the set of words over $\mathbb{Z}/N\mathbb{Z}$ of length l , $\bar{\mathcal{A}}^l = F_N^l \cap \bar{\mathcal{A}}$ and $\bar{\mathcal{C}}^l = F_N^l \cap \bar{\mathcal{C}}$. We first study the insertion and deletion in $\bar{\mathcal{A}}$.

Theorem 4.3. *If $w \in \bar{\mathcal{A}}^l$, then $\alpha w \in \bar{\mathcal{C}}^{l+1}$ and $w\alpha \in \bar{\mathcal{C}}^{l+1}$ for every $\alpha \in \mathbb{Z}/N\mathbb{Z}$.*

Proof. Assume that $w \in \bar{\mathcal{A}}^l$ and let $\alpha \in \mathbb{Z}/N\mathbb{Z}$. Then $\pi(w) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix}$ where $a \in \mathbb{Z}/N\mathbb{Z}$ and $b \in (\mathbb{Z}/N\mathbb{Z})^\times$. Thus

$$\pi(\alpha w) = \pi(\alpha)\pi(w) = \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} = \begin{bmatrix} -b^{-1} & 0 \\ -a - \alpha b^{-1} & -b \end{bmatrix}$$

and

$$\pi(w\alpha) = \pi(w)\pi(\alpha) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} = \begin{bmatrix} -b & a + \alpha b \\ 0 & -b^{-1} \end{bmatrix}.$$

Since $b \neq 0$, $\alpha w \in \bar{\mathcal{C}}^{l+1}$ and $w\alpha \in \bar{\mathcal{C}}^{l+1}$. □

Theorem 4.4. *Let $w \in \bar{\mathcal{C}}^l$ with $\pi(w) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$.*

(i) *If $\gcd(d, N) = 1$, i.e., $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, then there exist unique $\alpha, \beta \in \mathbb{Z}/N\mathbb{Z}$ such that $\alpha w \in \bar{\mathcal{A}}^{l+1}$ and $w\beta \in \bar{\mathcal{A}}^{l+1}$.*

(ii) *If $\gcd(d, N) > 1$, then $\alpha w \in \bar{\mathcal{C}}^{l+1}$ and $w\beta \in \bar{\mathcal{C}}^{l+1}$ for all $\alpha, \beta \in \mathbb{Z}/N\mathbb{Z}$.*

Proof. We first note that for $\alpha \in \mathbb{Z}/N\mathbb{Z}$,

$$\pi(\alpha w) = \pi(\alpha)\pi(w) = \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ -a + \alpha c & -b + \alpha d \end{bmatrix}.$$

Then $\alpha w \in \bar{\mathcal{A}}^{l+1} \Leftrightarrow -b + \alpha d \equiv 0 \pmod{N}$. This congruence equation has a solution $\Leftrightarrow \gcd(d, N) | b$. We claim that $\gcd(d, N) | b$ is equivalent to $\gcd(d, N) = 1$ and the theorem can easily be deduced. It is obvious that $\gcd(d, N) = 1$ implies $\gcd(d, N) | b$. If $\gcd(d, N) | b$, then $\gcd(d, N)$ is a common divisor of d and b . Since $ad - bc = 1$, $\gcd(d, N) \leq \gcd(d, b) = 1$, so $\gcd(d, N) = 1$. Hence we have the claim. □

Theorem 4.5. *If $\alpha_1 \dots \alpha_l \in \bar{\mathcal{A}}^l$, then $\alpha_2 \dots \alpha_l$ and $\alpha_1 \dots \alpha_{l-1} \in \bar{\mathcal{C}}^{l-1}$.*

Proof. Assume that $\alpha_1 \dots \alpha_l \in \bar{\mathcal{A}}^l$. Then $\pi(\alpha_1 \dots \alpha_l) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix}$ for some $a \in \mathbb{Z}/N\mathbb{Z}$ and $b \in (\mathbb{Z}/N\mathbb{Z})^\times$. Thus

$$\pi(\alpha_2 \dots \alpha_l) = \pi(\alpha_1)^{-1} \pi(\alpha_1 \dots \alpha_l) = \begin{bmatrix} \alpha_1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} = \begin{bmatrix} \alpha_1 a + b^{-1} & \alpha_1 b \\ a & b \end{bmatrix}$$

and

$$\pi(\alpha_1 \dots \alpha_{l-1}) = \pi(\alpha_1 \dots \alpha_l) \pi(\alpha_l)^{-1} = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} \begin{bmatrix} \alpha_l & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \alpha_l a + b & -a \\ -\alpha_l b^{-1} & b^{-1} \end{bmatrix}.$$

Since $b \neq 0$, $\alpha_2 \dots \alpha_l$ and $\alpha_1 \dots \alpha_{l-1} \in \bar{\mathcal{C}}^{l-1}$. □

Remark. We used to be able to derive the cardinalities of \mathcal{A}_r and \mathcal{C}_r by knowing the properties given in the above three theorem. However, in the finite ring $\mathbb{Z}/N\mathbb{Z}$ case is not the same as the finite field k case due to this ring contains zero divisors. This makes the words in F_N behave differently as we have seen in Theorem 4.4.

Another property of words in $\bar{\mathcal{A}}$ is given in the following theorem. This result will be used in the next section.

Theorem 4.6. $\alpha_1\alpha_2\ldots\alpha_l \in \bar{\mathcal{A}}^l$ if and only if $\alpha_l\alpha_{l-1}\ldots\alpha_1 \in \bar{\mathcal{A}}^l$.

Proof. Consider $\sigma = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\alpha_1\ldots\alpha_l \in F_N$ with $\pi(\alpha_1\ldots\alpha_l) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Since $\sigma \begin{bmatrix} w & x \\ y & z \end{bmatrix} \sigma = \begin{bmatrix} z & y \\ x & w \end{bmatrix}$ for all $w, x, y, z \in \mathbb{Z}/N\mathbb{Z}$ and $\sigma = \sigma^{-1}$, we have

$$\begin{aligned} \begin{bmatrix} d & c \\ b & a \end{bmatrix} &= \sigma\pi(\alpha_1\alpha_2\ldots\alpha_l)\sigma = (\sigma\pi(\alpha_1)\sigma)(\sigma\pi(\alpha_2)\sigma)\ldots(\sigma\pi(\alpha_l)\sigma) \\ &= \begin{bmatrix} \alpha_1 & -1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} \alpha_l & -1 \\ 1 & 0 \end{bmatrix} = \left(\begin{bmatrix} 0 & 1 \\ -1 & \alpha_l \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ -1 & \alpha_1 \end{bmatrix} \right)^{-1} \\ &= \pi(\alpha_l\ldots\alpha_1)^{-1}, \end{aligned}$$

so $\pi(\alpha_l\ldots\alpha_1) = \begin{bmatrix} a & -c \\ -b & d \end{bmatrix}$. Thus $\alpha_1\alpha_2\ldots\alpha_l \in \bar{\mathcal{A}}^l \Leftrightarrow d = 0 \Leftrightarrow \alpha_l\alpha_{l-1}\ldots\alpha_1 \in \bar{\mathcal{A}}^l$. \square

The partition $\bar{\mathcal{A}}$ and $\bar{\mathcal{C}}$ of F_k also induces the equivalence relation \sim on F_k . We record some relationships between two words in the next theorem.

Theorem 4.7. Let $x \in F_N$ and $\beta \in \mathbb{Z}/N\mathbb{Z}$. We have

- (i) If $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$, then $\alpha\beta x \sim (\beta - \alpha^{-1})x$.
- (ii) $0\beta x \sim x$.

Proof. Let $\pi(x) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

(i) Assume that $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$. Then

$$\pi(\alpha\beta x) = \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \beta \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a + \beta c & -b + \beta d \\ -\alpha a - c + \alpha\beta c & -\alpha b - d + \alpha\beta d \end{bmatrix}$$

and

$$\pi((\beta - \alpha^{-1})x) = \begin{bmatrix} 0 & 1 \\ -1 & \beta - \alpha^{-1} \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ -a + (\beta - \alpha^{-1})c & -b + (\beta - \alpha^{-1})d \end{bmatrix}.$$

Thus

$$\begin{aligned} \alpha\beta x \in \bar{\mathcal{A}} &\Leftrightarrow -\alpha b - d + \alpha\beta d = 0 \\ &\Leftrightarrow -b + (\beta - \alpha^{-1})d = 0 \\ &\Leftrightarrow (\beta - \alpha^{-1})x \in \bar{\mathcal{A}}, \end{aligned}$$

so $\alpha\beta x \sim (\beta - \alpha^{-1})x$.

(ii) Since $\pi(0\beta x) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \beta \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a + \beta c & -b + \beta d \\ -c & -d \end{bmatrix}$, $0\beta x \in \bar{\mathcal{A}} \Leftrightarrow d = 0 \Leftrightarrow x \in \bar{\mathcal{A}}$, so $0\beta x \sim x$. \square

Remark. The above theorem yields partial answers (again due to zero divisors in $\mathbb{Z}/N\mathbb{Z}$) for determination of words into classes $\bar{\mathcal{A}}$ and $\bar{\mathcal{C}}$. However, a good mathematical software such as MapleTM can easily compute the product of 2×2 matrices modulo positive integer N . This allows us to directly distinguish words in F_N .

5. MORE ON $\bar{\mathcal{A}}$

We concentrate more on $\bar{\mathcal{A}}$ and record its further parallel properties to Bacher's in this last section. This work includes unique factorization, predecessors, successors and periodic words.

In order to prove the fact about unique factorization on $\bar{\mathcal{A}}$, we start with the following lemma.

Lemma 5.1. (i) If $w, w' \in \bar{\mathcal{A}}$ then $ww' \in \bar{\mathcal{C}}$ and $w\alpha w' \in \bar{\mathcal{A}}$ for any $\alpha \in \mathbb{Z}/N\mathbb{Z}$.
(ii) If exactly one of w, w' is an element of $\bar{\mathcal{A}}$ then $w\alpha w' \in \bar{\mathcal{C}}$ for any $\alpha \in \mathbb{Z}/N\mathbb{Z}$.

Proof. To prove (i), let $\pi(w) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix}$ and $\pi(w') = \begin{bmatrix} a' & b' \\ -b'^{-1} & 0 \end{bmatrix}$ for some $a, a' \in \mathbb{Z}/N\mathbb{Z}$, $b, b' \in (\mathbb{Z}/N\mathbb{Z})^\times$, and let $\alpha \in \mathbb{Z}/N\mathbb{Z}$. Then

$$\pi(ww') = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} \begin{bmatrix} a' & b' \\ -b'^{-1} & 0 \end{bmatrix} = \begin{bmatrix} aa' - bb'^{-1} & ab' \\ -a'b^{-1} & -b^{-1}b' \end{bmatrix},$$

and

$$\pi(w\alpha w') = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} \begin{bmatrix} a' & b' \\ -b'^{-1} & 0 \end{bmatrix} = \begin{bmatrix} -ba' - ab'^{-1} - \alpha bb'^{-1} & -bb' \\ (bb')^{-1} & 0 \end{bmatrix}.$$

Thus $w\alpha w' \in \bar{\mathcal{A}}$ for any $\alpha \in \mathbb{Z}/N\mathbb{Z}$. Since $b, b' \in (\mathbb{Z}/N\mathbb{Z})^\times$, $ww' \in \bar{\mathcal{C}}$.

To prove (ii), suppose that $w \in \bar{\mathcal{A}}$ and $w' \in \bar{\mathcal{C}}$ and let $\alpha \in \mathbb{Z}/N\mathbb{Z}$. Then $\pi(w) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix}$ for some $a \in \mathbb{Z}/N\mathbb{Z}$ and $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, and $\pi(w') = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ in $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ with $d' \neq 0$. Thus

$$\pi(w\alpha w') = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} -ba' + ac' + \alpha bc' & -bb' + ad' + \alpha bd' \\ -b^{-1}c' & -b^{-1}d' \end{bmatrix}.$$

Since $b \in (\mathbb{Z}/N\mathbb{Z})^\times$ and $d' \neq 0$, $w\alpha w' \in \bar{\mathcal{C}}$. For another case, let $w = \beta_1 \dots \beta_m \in \bar{\mathcal{C}}$ and $w' = \beta'_1 \dots \beta'_n \in \bar{\mathcal{A}}$ for some positive integers m and n . By Theorem 4.6, we have $\beta'_n \dots \beta'_1 \in \bar{\mathcal{A}}$ and $\beta_m \dots \beta_1 \in \bar{\mathcal{C}}$. The previous proof shows that

$$\beta'_n \dots \beta'_1 \alpha \beta_m \dots \beta_1 \in \bar{\mathcal{C}}.$$

Thus we get $w\alpha w' = \beta_1 \dots \beta_m \alpha \beta'_1 \dots \beta'_n \in \bar{\mathcal{C}}$ by Theorem 4.6. \square

Let $\mathcal{P}^l = \{\alpha_1 \alpha_2 \dots \alpha_l \in \bar{\mathcal{A}}^l : \alpha_1 \dots \alpha_h \in \bar{\mathcal{C}}^h \text{ for } h = 1, \dots, l-1\}$ and $\mathcal{P} = \bigcup \mathcal{P}^l$.

Theorem 5.2. [Unique Factorization in $\bar{\mathcal{A}}$] Let $w \in F_N$. Then $w \in \bar{\mathcal{A}}$ if and only if w can be written as

$$w = p_1 \delta_1 p_2 \delta_2 \dots p_n \delta_n p_{n+1}$$

for some $n \geq 0$ with $p_1, \dots, p_{n+1} \in \mathcal{P}$ and $\delta_1, \dots, \delta_n \in \mathbb{Z}/N\mathbb{Z}$. Moreover, such a factorization of $w \in \bar{\mathcal{A}}$ is unique.

Proof. Suppose that w can be written as in this form. By Lemma 5.1, it is easy to see that $w \in \bar{\mathcal{A}}$. Conversely, assume that $w = \alpha_1 \alpha_2 \dots \alpha_l \in \bar{\mathcal{A}}^l$. Then there is the smallest positive integer s such that $\alpha_1 \dots \alpha_s \in \bar{\mathcal{A}}$. Setting $p_1 = \alpha_1 \dots \alpha_s \in \mathcal{P}$ and $\delta_1 = \alpha_{s+1}$. Thus $\alpha_{s+2} \alpha_{s+3} \dots \alpha_l$ must be in $\bar{\mathcal{A}}^{l-(s+1)}$ by Lemma 5.1. Repeating this process we get the sets $\{\delta_1, \dots, \delta_n\} \subset \mathbb{Z}/N\mathbb{Z}$ and $\{p_1, \dots, p_{n+1}\} \subset \mathcal{P}$ so that $w = p_1 \delta_1 p_2 \delta_2 \dots p_n \delta_n p_{n+1}$ for some $n \geq 0$. The smallest length of p_i for each i implies the uniqueness of this factorization. \square

Given two words $w, w' \in F_N$ of the form

$$w = \alpha_0 \alpha_1 \dots \alpha_{l-1} \quad \text{and} \quad w' = \alpha_1 \alpha_2 \dots \alpha_l,$$

we call w' an *immediate successor* of w and w an *immediate predecessor* of w' .

Theorem 5.3. *Each element $w \in \bar{\mathcal{A}}^l$ has a unique immediate successor and a unique immediate predecessor in $\bar{\mathcal{A}}^l$.*

Proof. Assume that $\alpha_0 \alpha_1 \dots \alpha_{l-1} \in \bar{\mathcal{A}}^l$. Then $\pi(\alpha_0 \alpha_1 \dots \alpha_{l-1}) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix}$ for some $a \in \mathbb{Z}/N\mathbb{Z}$ and $b \in (\mathbb{Z}/N\mathbb{Z})^\times$. Thus

$$\begin{aligned} \pi(\alpha_1 \alpha_2 \dots \alpha_{l-1}) &= \pi(\alpha_0)^{-1} \pi(\alpha_0 \alpha_1 \dots \alpha_{l-1}) \\ &= \begin{bmatrix} \alpha_0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} = \begin{bmatrix} \alpha_0 a + b^{-1} & \alpha_0 b \\ a & b \end{bmatrix}, \end{aligned}$$

so

$$\begin{aligned} \pi(\alpha_1 \alpha_2 \dots \alpha_l) &= \pi(\alpha_1 \alpha_2 \dots \alpha_{l-1}) \pi(\alpha_l) \\ &= \begin{bmatrix} \alpha_0 a + b^{-1} & \alpha_0 b \\ a & b \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \alpha_l \end{bmatrix} = \begin{bmatrix} -\alpha_0 b & \alpha_0 a + b^{-1} + \alpha_0 \alpha_l b \\ -b & a + \alpha_l b \end{bmatrix}. \end{aligned}$$

Since $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, $\alpha_1 \alpha_2 \dots \alpha_l \in \bar{\mathcal{A}}^l \Leftrightarrow \alpha_l = -ab^{-1}$. Hence w has a unique immediate successor in $\bar{\mathcal{A}}^l$. Similarly, we can show that w also has a unique immediate predecessor in $\bar{\mathcal{A}}^l$. \square

For $w = \alpha_1 \alpha_2 \dots \alpha_l \in \bar{\mathcal{A}}^l$, by Theorem 5.3 there exists an infinite word

$$W = \dots \alpha_{-1} \alpha_0 \alpha_1 \alpha_2 \alpha_3 \dots$$

such that $\alpha_{i+1} \dots \alpha_{i+l}$ is the immediate successor in $\bar{\mathcal{A}}^l$ of $\alpha_i \dots \alpha_{i+l-1}$ for all integer i . That is, all subwords formed by l consecutive letters of W are elements in $\bar{\mathcal{A}}^l$. Since $\bar{\mathcal{A}}^l$ is finite, the infinite word W associated to w is periodic. Hence for every $w \in \bar{\mathcal{A}}^l$, there exists the smallest positive integer s such that the infinite word W associated to w is s -periodic.

Example 5.4. Some infinite periodic words over $\mathbb{Z}/6\mathbb{Z}$.

- (1) The infinite periodic word corresponding to both 121 and 212 is a 2-periodic word $\dots 1212 \dots$
- (2) The infinite periodic word corresponding to 234, 343 and 432 is a 4-periodic word $\dots 23432343 \dots$

Theorem 5.5. *Let $W = \dots \alpha_{s-1} \alpha_0 \alpha_1 \dots \alpha_{s-1} \alpha_0 \alpha_1 \dots$ be an infinite s -periodic word with letters in $\mathbb{Z}/N\mathbb{Z}$. Then there exists a smallest positive integer t such that all subwords of length $ts - 1$ in W belong to $\bar{\mathcal{A}}$. Moreover, all subwords of length $lts - 1$ ($l \geq 1$) of W belong to $\bar{\mathcal{A}}$.*

Proof. We observe that the elements

$$\pi(\alpha_0 \alpha_1 \dots \alpha_{s-1}), \pi(\alpha_1 \dots \alpha_{s-1} \alpha_0), \dots, \pi(\alpha_{s-1} \alpha_0 \dots \alpha_{s-2}) \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

are all conjugate. Then they have a common order t' , we claim that t' has the desired property. Let w be a subword of length $t's$ in W . Thus $w = \underbrace{w'w' \dots w'}_{t' \text{ copies}}$ where w' is a subword of length s in W , so

$$\pi(w) = \pi(\underbrace{w'w' \dots w'}_{t' \text{ copies}}) = (\pi(w'))^{t'} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Assume that $w = \beta_1 \dots \beta_{t's}$. The subword of length $t's - 1$ associated with w is in $\bar{\mathcal{A}}$ as a result of $\pi(\beta_1 \dots \beta_{t's-1}) = \pi(w) \pi(\beta_{t's})^{-1} = \begin{bmatrix} \beta_{t's} & -1 \\ 1 & 0 \end{bmatrix}$. Hence $t \leq t'$ exists by the well-ordering principle. \square

Remark. In the above proof, sometimes $t < t'$. For example, consider the infinite 1-periodic word, $\dots 000 \dots$. The order of $\pi(0) = 4$ but we can choose $t = 2$ since $0 \in \bar{\mathcal{A}}$. Moreover, since t' divides $|\text{SL}_2(\mathbb{Z}/N\mathbb{Z})|$, we know that $t \leq |\text{SL}_2(\mathbb{Z}/N\mathbb{Z})|$.

Example 5.6. In $\mathbb{Z}/6\mathbb{Z}$, consider the 4-periodic word $W = \dots 23432343 \dots$

(1) We have $t = 1$ so that all subwords of length $4(1) - 1 = 3$ in W belong to $\bar{\mathcal{A}}$.

(234, 343, 432, 323)

(2) For $l = 2$, all subwords of length $4(2) - 1 = 7$ in W belong to $\bar{\mathcal{A}}$.

(2343234, 3432343, 4323432, 3234323)

(3) For $l = 3$, all subwords of length $4(3) - 1 = 11$ in W belong to $\bar{\mathcal{A}}$.

(23432343234, 34323432343, 43234323432, 32343234323)

REFERENCES

- [B00] R. Bacher, *An equivalence relation on $\{0, 1\}^*$* , Europ. J. Combinatorics, **21** (2000), 853-864.
- [B02] R. Bacher, *$SL_2(k)$ and a subset of words over k* , Europ. J. Combinatorics, **23** (2002), 141-147.
- [S73] J.-P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973.

YOTSANAN MEEMARK, DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE, CHULALONGKORN UNIVERSITY, BANGKOK, 10330 THAILAND

E-mail address: yotsanan.m@chula.ac.th

TASSAWEE THITIPAK, DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE, CHULALONGKORN UNIVERSITY, BANGKOK, 10330 THAILAND

E-mail address: thitipakt@gmail.com